UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/606,130	06/24/2003	Mithat C. Dogan	15685P211	4022

45222 7590 09/20/2005

ARRAYCOMM/BLAKELY
12400 WILSHIRE BLVD
SEVENTH FLOOR
LOS ANGELES, CA 90025-1030

EXAMINER	
DINH, MINH	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 09/20/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/606,130	DOGAN ET AL.	
	Examiner	Art Unit	
	Minh Dinh	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 June 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3,9,11-20,26-28,34,36 and 37* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3,9,11-20,26-28,34,36 and 37* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *24 June 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *7/22/2005*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This action is in response to the amendment filed 06/27/2005. Claims 1, 9, 14, 26 and 34 have been amended; claims 4-8, 10, 21-25, 29-33 and 35 have been cancelled.

2. The objection to claim 37 in the previous Office Action has not been addressed in the amendment. Applicant is reminded to respond to the objection in the next reply.

Response to Arguments

3. Applicant's arguments filed 06/27/2005 have been fully considered but they are not persuasive. Applicants argue that "3G Security" does not teach: sending a random access connection request burst from the first communication device to the second communications device, opening a connection between the first communications device and the second communications device in response to the random access connection request burst, generating an initialization vector using an absolute frame number of the random access connection request burst, and determining a connection secret using the master secret and the initialization vector (page 10). "3G Security" discloses an encryption method used in a mobile telecommunication system to protect data transmitted from a user equipment (UE) to a radio network controller (RNC). In particular, "3G Security" discloses generating an initialization vector COUNT-C, and determining a connection secret using a master secret CK and COUNT-C (fig. 16b,

page 36). "3G Security" further discloses that COUNT-C or ciphering sequence number (CSN) is identical to the UEFN (user equipment frame number), and includes a CFN (Section 6.6.4.1 COUNT-C, page 37). The CFN is the connection frame number, and therefore, meets the limitation of an absolute frame number of the random access connection request.

Claim Objections

4. Claim 37 is objected to because of the following informalities: claim 37 is a machine-readable medium depending on claim 2, which is a method claim. It's considered that "claim 2" is a typo error. For examination purpose, claim 37 is treated as being depended upon claim 27. Appropriate correction is required.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

6. Claims 1-3, 11-12, 14-20, 26-28 and 36-37 are rejected under 35 U.S.C. 102(b) as being anticipated by "3G TS 33.102 V3.4.0 - 3G Security - Security Architecture" (hereinafter "3G Security").

Regarding claim 1, which is exemplary of claims 14-15 and 26, "3G Security" discloses a method comprising: establishing a master secret between a first communications device and a second communications device (fig. 16b, p. 36; Section 6.6.4.2 CK, p. 37-38); sending a random access connection request burst from the first device to the second device (Section 6.4.5 Security mode set-up procedure, p. 30-31); opening a connection between the first communications device and the second communications device in response to the random access connection request burst; generating an initialization vector COUNT-C using the CFN which meets the limitation of an absolute frame number of the random access connection request burst, and determining a connection secret using the master secret and the initialization vector; and using the connection secret for symmetric key cryptography during the connection (fig. 16b, p. 36; Section 6.6.3 Ciphering method – 6.6.4 Input Parameters to the cipher algorithm, p. 36-38).

Regarding claims 2, 16-17 and 27, "3G Security" further discloses initializing a cipher using the connection secret; and sending one or more bursts over the connection, the one or more bursts carrying data encrypted using the initialized cipher (Section 6.6.3 Ciphering method, p. 36-37).

Regarding claims 3, 18-20 and 28, "3G Security" further discloses initializing a cipher using the connection secret; receiving one or more bursts over the connection, the one or more bursts carrying data encrypted using the initialized cipher; and decrypting the data using the initialized cipher (Section 6.6.3 Ciphering method, p. 36-37).

Regarding claims 11-12 and 36-37, "3G Security" further discloses that the connection comprises a communications stream and that the cipher comprises a stream cipher (fig. 16b, p. 36).

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 9 and 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over "3G Security" as applied to claims 1 and 26 above, and further in view of Niemi et al (2002/0035682). "3G Security" does not disclose that the first communications device does not sent the initialization vector to the second communications device. Niemi discloses an encryption method utilizing an initialization vector. Niemi further discloses that a first communications device does not sent the initialization vector to a second communications device (fig. 4; paragraph 0069). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the "3G Security" method such that the first communications device does not sent the initialization vector to the second communications device, as taught by Niemi, in order to save transmission bandwidth.

9. Claim 13 is rejected under 35 U.S.C. 103(a) as being unpatentable over "3G Security" as applied to claim 12 above, and further in view of Skantze (2002/0035687). "3G Security" does not disclose using RC4 cipher. Skantze discloses using RC4 cipher in wireless transmission (paragraph [0140]). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the "3G Security" method to use RC4 cipher, as taught by Skantze. RC4 cipher is a relative fast and strong cipher.

Conclusion

10. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

U.S. Patent No. 6,909,887 to Fauconnier et al.

U.S. Patent Application Publication No. 2003/0044011 to Vialen et al.

U.S. Patent Application Publication No. 2004/0004947 to Herrmann et al.

Technical Specification 3G TS 25.401 v1.1.1 (1999-07) - UTRAN Overall Description

11. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dinh whose telephone number is 571-272-3802. The examiner can normally be reached on Mon-Fri: 10:00am-6:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MD

Minh Dinh
Examiner
Art Unit 2132

MD
9/16/05

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100